4.

JÄTÄ VÄHEMMÄN JÄLKIÄ

Puhelimesi selain tallentaa paljon tietoa sinusta: sijaintisi, hakusi ja käyttämäsi verkkosivustot. Se saattaa myös antaa nämä tiedot eteenpäin.

Voit palauttaa joidenkin tietojen hallinnan tekemällä muutamia muutoksia.

Puhelimiin, tabletteihin ja tietokoneisiin on yleensä esiasennettu selaimet, jotka eivät priorisoi tietosuojaasi. Sen sijaan voit ladata ja käyttää selainta, joka suojaa oletusarvoisesti verkkotoimintaasi seuraajilta.

Joihinkin lisättyihin tietosuojaimiin voi asentaa lisäosia ja laajennuksia (nämä ovat selaimeesi helposti asennettavia pienoisohjelmia, jotka voivat lisätä verkkotoimintasi tietosuojaa).

5.

POISTA OMAT JA MUIDEN TUNNISTEET

Oletko kerryttänyt myös ystäviesi tietoja merkitsemällä heitä valokuviin ja viesteihin?

Kevennä heidän tietokuormitustaan (ja samalla omaatuntoasi) **poistamalla merkinnät** niin monista valokuvista ja viesteistä kuin mahdollista.

Välitä viestiä! Kannusta ystäviäsi, perhettäsi ja työtovereitasi hallitsemaan omia tietojaan. Jos me kaikki hallitsemme omia tietojälkiämme, voimme paremmin auttaa toisiamme tietopuhdistuksessa.

Tuotteen takana

TACTICAL TECH

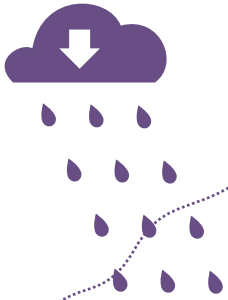
Tukijana

Firefox

datadetoxkit.org
#datadetox

Estä vakoilumainokset ja näkymätön seuranta asentamalla uBlock Origin (Chromeen, Safariin tai Firefoxiin) tai Privacy Badger (Chromeen, Firefoxiin tai Operaan).

Varmista, että yhteydet verkkosivustoihin ovat mahdollisuuksien mukaan turvallisia, asentamalla HTTPS Everywhere: selainlaajennus. Se takaa, että viestintäsi monien suurten verkkosivustojen kanssa on salattu ja suojattu tiedonsiirron aikana. Jos olet Safarin käyttäjä ja haluat hyödyntää tätä ominaisuutta, aseta oletushakukoneeksi jokin muu kuin Googlen tuote, kuten DuckDuckGo, joka ohjaa sinut salattuihin yhteyksiin automaattisesti.



DATA DETOX KIT

HALLITSE ÄLYPUHELIMESI TIETOJA

parantaaksesi tietosuojaasi verkossa

Sinusta saattaa tuntua, ettei sillä ole juurikaan väliä, mitä tietosi kertovat sinusta muille. Ketä kiinnostaa, että pidät kantrimusiikista tai että haluaisit ostaa kenkiä yli tarpeesi tai aloittaa seuraavan loman suunnittelemisen jo vuotta aiemmin?

Ongelma on siinä, mitä tiedoillesi tapahtuu. Ajan myötä tiedoista nimittäin muodostuu intiimi digitaalinen malli. Tottumuksesi, liikkeesi, suhteesi, mieltymyksesi, uskomuksesi ja salaisuutesi paljastetaan niille, jotka analysoivat tietojasi ja hyötyvät niistä. Tällaisia tahoja saattavat olla esimerkiksi yritykset ja tiedonvälittäjät.

Lukemalla lisää Data Detox -puhdistuskuurista saat tietää, miten ja miksi näin tehdään, ja voit ryhtyä käytännön toimiin eli hallitsemaan verkkoon jättämiäsi tietojälkiä.

Aloitetaan!

1.

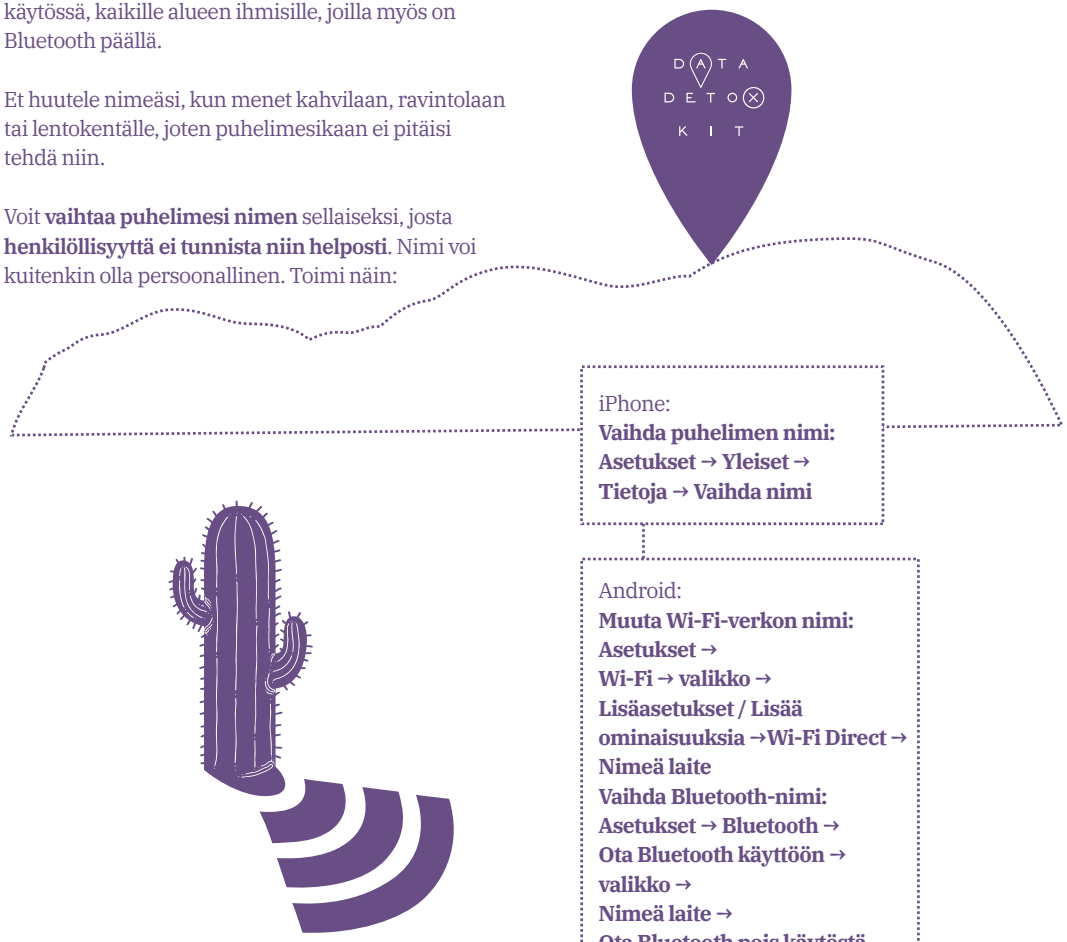
MUUTA LAITTEESI NIMI

Jossain vaiheessa olet saattanut ”nimetä” puhelimesi Wi-Fiä, Bluetoothia tai molempia varten – tai ehkä nimi luotiin automaattisesti puhelimen ensimmäisen asennuksen aikana.

Tämä tarkoittaa, että ”Kalle Virtasen puhelin” näkyy Wi-Fi-verkon omistajalle ja, jos Bluetooth on käytössä, kaikille alueen ihmisille, joilla myös on Bluetooth päällä.

Et huutele nimeäsi, kun menet kahvilaan, ravintolaan tai lentokentälle, joten puhelimesikaan ei pitäisi tehdä niin.

Voit **vaihtaa puhelimesi nimen** sellaiseksi, josta **henkilöllisyyttä ei tunnista niin helposti**. Nimi voi kuitenkin olla persoonallinen. Toimi näin:



iPhone:
Vaihda puhelimen nimi:
Asetukset → Yleiset →
Tietoja → Vaihda nimi

Android:
Muuta Wi-Fi-verkon nimi:
Asetukset →
Wi-Fi → valikko →
Lisäasetukset / Lisää ominaisuuksia →Wi-Fi Direct →
Nimeä laite
Vaihda Bluetooth-nimi:
Asetukset → Bluetooth →
Ota Bluetooth käyttöön →
valikko →
Nimeä laite →
Ota Bluetooth pois käytöstä

2.

PYYHI SIJAINTISI JALANJÄLJET

Vaikka saattaakin näyttää siltä, että sijaintitietosi ovat vain satunnaisia tiedonmurusia, yhdessä ne voivat paljastaa tärkeitä tietoja sinusta ja tottumuksistasi, kuten asuinpaikastasi, työpaikastasi ja siitä, missä haluat viettää aikaa ystäviesi kanssa. Siksi nämä tiedot ovatkin haluttua tavaraa monille yrityksille ja tiedonvälittäjille.

Voit käydä läpi kunkin sovelluksen käyttöoikeudet ja ottaa sijaintipalvelut pois käytöstä. Etsi sovelluksia, jotka eivät todellakaan tarvitse näitä tietoja palvelujaan varten (tarvitseeko kyseisen pelin todella tietää missä olet?) ja niitä sovelluksia, joiden et halua tietävän liikkeistäsi.

Android:
Asetukset →Sovellukset →
Valitse sijainnin käyttö sovelluskohtaisesti

iPhone:
Asetukset → Tietosuoja →
Sijaintipalvelut →
Valitse sijainnin käyttö sovelluskohtaisesti

3.

SIIVOA SOVELLUKSESI

Sosiaalisen median sovellukset, pelit ja sääsovellukset ovat kiinnostuneita tiedoistasi, ja ne saattavatkin kerätä niitä melko paljon.

Poistamalla satunnaiset sovellukset, joita et koskaan käytä, voit tehokkaasti puhdistaa digitaalista identiteettiäsi.

Turhien sovellusten siivoaminen myös vapauttaa tilaa puhelimestasi, vähentää datan käyttöä ja pidentää akun käyttöikää. Näin voit jopa – sovelluksesta riippuen – lisätä puhelimen yleistä suorituskykyä.

Android:
Asetukset → Sovellukset →
Valitse sovellus, jonka haluat poistaa → Poista

iPhone:
Pidä sovelluskuvaketta painettuna, kunnes valikko tulee näkyviin.

Valitse listalta kohta Poista sovellus.

Vahvista sovelluksen poisto.

4.

SUOJAA VIRTUAALISET ARVOTAVARASI

Aivan kuten pidät huolta kotisi arvotavaroista, sinun tulee huolehtia myös virtuaalisesti tallentamistasi tiedoista, olipa kyse sitten pankkitiedoista, skannatusta passista, osoitteesta tai puhelinnumerosta. Kannattaa miettiä, mihin tallennat arvokkaimmat henkilötietosi, ja kuinka voit suojata niitä.

Pikapuhdistus on hyvä kikka, jos haluat tehdä muutamia nopeita parannuksia vaikkapa kahvitauolla. Etsi tiettyjä tietoja, jotka löytyvät sähköpostistasi tai muilta tileiltäsi, ja poista ne. Ota kohteeksi esimerkiksi skannattu henkilötodistus, pankkitiedot tai sairausvakuutustiedot. Jos tarvitset tietoja myöhemmin, voit aina ladata tiedot tai tulostaa ne ennen kuin poistat ne sähköpostitililtäsi.

Syväpuhdistus on perusteellisempi tapa, ja se on hyvä tehdä kerran vuodessa. Arkistoi kaikki tiedot sähköpostistasi tai sosiaalisen median tileiltä, lataa tiedot tietokoneellesi ja poista tilien sisältö aloittaaksesi uudelleen puhtaalta pöydältä.

Vinkki: Älä pelkästään poista. Tyhjennä myös roskakori ja tilapäiset tiedostot!

Voit itse valita, haluatko varmuuskopioida arkistot ja asiakirjat pilveen vai tallentaa ne ulkoiselle kiintolevylle tai USB-tikulle. Huolimatta siitä, miten tallennat, varmista, ettet menetä tietoja ja että salasanasi on vahva ja muistissasi.

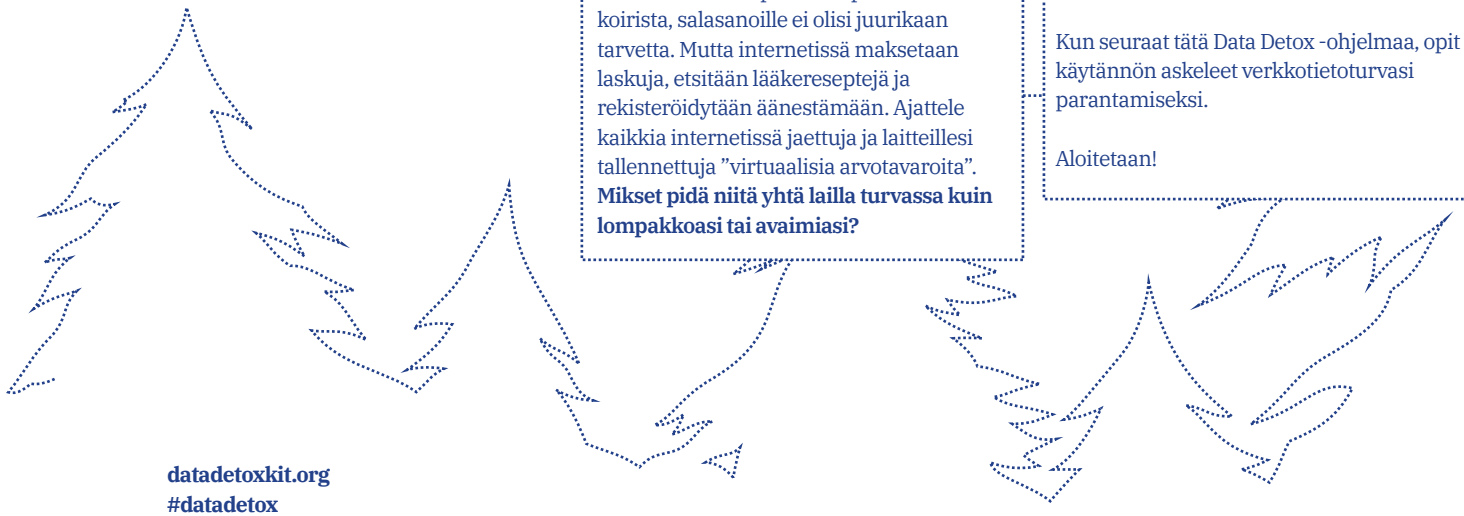
5.

VÄLITÄ VIESTIÄ!

On ehkä helppo unohtaa, että verkkoa kutsutaan ”verkoksi” syystä. **Olemme kaikki yhteydessä verkkoon** eri verkostojen kautta, ei vain ystävinä sosiaalisessa mediassa, vaan myös sähköpostitiliemme yhteystietojen ja verkossa jakamiemme valokuvien kautta. Kun suojaat tilisi, vahvistat salasanasi ja puhdistat tietosi, sinun lisäksesi myös muut hyötyvät. Toimintasi auttaa pitämään jokaisen, johon olet yhteydessä, hieman paremmassa turvassa.

Kun puhdistat sähköpostiasi ja sosiaalisen median tilejäsi, mieti, mitä muuta voisit poistaa ystäviäsi tai työtovereitasi auttaaksesi. Sisaresi pankkitiedot, toimistosi avainkoodi tai poikasi passin kopio ovat vain muutamia esimerkkejä tiedoista, joiden päätyminen vääriin käsiin voi aiheuttaa melkoista päänsärkyä.

Välitä viestiä! Digitaalisen turvallisuuden lisääminen on helppoa muutamaa perusvaihetta noudattamalla. Jaa tämä Data Detox ystävien, perheen tai työtovereidesi kanssa, jotta myös he voivat muuttaa tapojaan järkevällä tavalla.



DATA DETOX KIT

VAIHDA ASETUKSIASI

tietojesi turvaamiseksi

Jos internet olisi vain paikka, jossa jaetaan kuvia dinosauruspukuihin puetuista koirista, salasanoille ei olisi juurikaan tarvetta. Mutta internetissä maksetaan laskuja, etsitään lääkereseptejä ja rekisteröidytään äänestämään. Ajattele kaikkia internetissä jaettuja ja laitteillesi tallennettuja ”virtuaalisia arvotavaroita”. **Mikset pidä niitä yhtä lailla turvassa kuin lompakkoasi tai avaimiasi?**

On yksi yksinkertainen tapa vaikeuttaa muiden pääsyä virtuaalitavaroihisi: **älä tee salasanojen arvaamisesta liian helppoa.** Suurin osa ihmisistä ei tarvitse erityisiä teknisiä taitoja päästäkseen tileillesi. Tarvitaan vain muutama arvaus salasanoistasi tai automaattinen ohjelma.

Kun heillä on pääsy yhdelle tilille, he voivat kokeilla vaarantunutta salasanaa muille tileille, kerätä tietoja sinusta ja tottumuksistasi, ottaa haltuun omistamasi tilit tai jopa käyttää digitaalista identiteettiäsi.

Kun seuraat tätä Data Detox -ohjelmaa, opit käytännön askeleet verkkotietoturvasi parantamiseksi.

Aloitetaan!

Tuotteen takana
TACTICAL TECH

Tukijana
Firefox

datadetoxkit.org
#datadetox

1.

LUKITSE DIGITAALINEN OVESI

Laitteesi näytönlukitukset eli salasana, kuvio, sormenjälki tai kasvotunnistus ovat *parhaita suojautumiskeinoja sellaisia henkilöitä vastaan, jotka haluavat päästä käsiksi laitteeseesi. Lukituskeinoja on useita erilaisia, ja voi olla vaikea tietää, mikä niistä sopii parhaiten juuri sinulle.

Mikä tahansa lukitus puhelimessa, tabletissa tai tietokoneessa antaa sinulle paremman suojan kuin ei lukitusta ollenkaan. Ja aivan kuten erilaiset oveen laitettavat lukot, **jotkut näytönlukitukset ovat vahvempia kuin toiset.**

Vahvimpia ovat pitkät, yksilölliset salasanat. Jos käytät lukituksen avaamiseen salasanaa, sen tulisi sisältää kirjaimia, numeroita ja erikoismerkkejä.

Jos nykyisin avaat puhelimesi pyyhkäisemällä, voit lisätä tietoturvaasi asettamalla puhelimeesi pitkän salasanan. Vai käytätkö kuviolukitusta? Entä jos muuttaisit kuvion hiukan pidemmäksi? Onko PIN-koodisi 1234? Entä jos valitsisit uuden PIN-koodin pyöräyttämällä noppaa seitsemän kertaa ja pistämällä tuon koodin mieleesi helpon koodin sijasta? **Pieni muutos voi olla iso askel kohti laitteidesi parempaa hallintaa.**

2.

PÄÄSTÄ SISÄÄN VAIN HARVAT JA VALITUT

Huipputason salasanojen luominen on helppoa. Sinun tarvitsee vain noudattaa muutamia perusperiaatteita. Salasanan tulee olla:

Pitkä: **salasanoissa tulee olla vähintään kahdeksan merkkiä. Vielä vahvempi? 16–20 merkkiä**

Ainutlaatuinen: **jokaisen käyttämäsi salasanan – jokaisella sivustolla – tulisi olla erilainen**

Satunnainen: **salasanasi ei tulisi olla looginen eikä helposti arvattavissa. Salasanojen hallintaohjelmista on paljon hyötyä.**

Vahvimmissa salasanoissa yhdistellään kirjaimia, numeroita ja erikoismerkkejä. Tämä vanha neuvo toimii, ja sen avulla rakennat vahvemman ja vaikeammin arvattavan salasanan. Jotkin salasanajärjestelmät eivät valitettavasti anna käyttää erikoismerkkejä (kuten @ # $% - = +), mutta riittävän pitkä kirjainten ja numeroiden yhdistelmä on silti parempi kuin lyhyt.

Parasta tapa on käyttää **erillistä salasananhallintaa** kaikkien salasanojen luomiseen ja tallentamiseen. Turvallisuusasiantuntijoiden suosittelemat salasanojen hallintaohjelmat, kuten 1Password ja KeePassXC, ovat sovelluksia, joiden ainoa tarkoitus on suojata kirjautumistunnuksesi ja muita arkaluonteisia tietoja.

3.

LISÄÄ TOINEN AVAIN

Kaksivaiheisen todennuksen (two-factor authentication, 2FA) tai monivaiheisen todennuksen (multifactor authentication, MFA) asettaminen tarkoittaa, että vaikka joku löytäisi salasanasi, **hänellä ei todennäköisesti olisi tiedossa toista avainta, jota tarvitaan laitteen avaamiseen.**

Tutustu eniten käyttämiesi sivustojen ja sovellusten suojausasetuksiin nähdäksesi, voitko määrittää ylimääräisen avaimen. Aloita tärkeimmistä: kaikki pankkisovellukset tai sähköpostin kaltaiset palvelut, joita käytät muiden tiliesi palauttamiseen.

Google:
Kirjaudu sisään osoitteeseen myaccount.google.com → Tietoturva → 2-vaiheinen vahvistus → Aloita

Facebook:
valikko → Asetukset → Turvallisuus ja sisäänkirjautuminen → Käytä kaksivaiheista todennusta

Vinkki: Kun määrität uutta vahvistustasoa, sinun on valittava toinen tapa vahvistaa henkilöllisyytesi. Yritä välttää (puhelinnumeroosi lähetettävien) tekstiviestien käyttöä siltä varalta, että kadotat puhelimesi. Sähköposti on yleensä luotettavampi vaihtoehto.

4.

ANNA ÄÄNESI KUULUA

Jos et ole tyytyväinen usein käyttämiesi verkkosivustojen tai sovellusten riippuvuutta aiheuttaviin tai suostutteleviin toimintoihin tai väärään tietoon, voit lähettää yrityksille sähköposteja tai kirjoittaa twiittejä ja kertoa, ettet ole samaa mieltä heidän käytäntöjensä kanssa. Kun yritysten arvokkain omaisuus eli niiden käyttäjät painostavat yrityksiä ryhtymään toimiin, ne saattavat jopa muuttua.

Jos sinusta tuntuu, ettei palautteeseesi reagoida, voit tehdä jotain todella tehokasta: käyttää toista verkkosivustoa tai sovellusta. Jos olet kertonut, että olet tyytymätön jonkin verkkosivuston tai sovelluksen toimintaan, lopetat sen käytön tai poistat asennuksen – ja tarpeeksi monet muut tekevät samoin – **yritykset huomaavat sen kyllä.**

5.

LEVITÄ SANAA

Välitä tietoa! Tämä vinkki on helppo unohtaa, mutta sillä voi olla suuri vaikutus. Kerro ystävillesi, perheellesi ja työtovereillesi huomaamistasi asioista ja pyydä heitä liittymään mukaan puhdistuskuurille!

Kaikki kamppailevat puhelintottumustensa kanssa. On tärkeää löytää tapa, joka tuntuu juuri sinulle sopivalta ja sopii elämäntyyliisi. Kokeile, kunnes löydät itsellesi sopivat käytännöt ja päivitä tapojasi ajan myötä. Yhtä ja ainoaa, kaikille sopivaa ratkaisua ei ole olemassa.

Ja lopuksi: kerro valinnoistasi läheisillesi. Jos esimerkiksi olet päättänyt olla käyttämättä Messenger-sovellusta päivittäin kello 20 jälkeen, koska silloin vietät näyttövapaata aikaa: kerro siitä perheellesi ja ystävillesi, jotta he voivat tarvittaessa soittaa sinulle.

Pidä vuoropuhelu avoimena, kysy kysymyksiä ja voit elää sinulle sopivaa tasapainoista verkkoelämää.

DATA DETOX KIT

VAIHDA OLETUSASETUKSIA

parantaaksesi digitaalista hyvinvointiasi

Milloin viimeksi ”irrottauduit verkosta” etkä koskenut teknisiin laitteisiin koko päivänä tai edes yhden tunnin aikana? Jos teet jotakin niin usein, haluat sen varmasti olevan aikasi arvoista. Kuinka voit varmistaa, että laitteella käyttämäsi aika on laatuaikaa?

Ensiksikin on hyvä muistaa, että tekniikan vastustamaton vetovoima ei ole sinun syytäsi! Usko tai älä, suosikkisovelluksesi ja -verkkosivustosi on suunniteltu siten, että jokainen ominaisuus, väri ja ääni on optimoitu pitämään sinut koukussa, myymään ja saamaan sinut palaamaan aina takaisin.

Haluatko löytää terveellisemmän tasapainon verkkoelämän ja offline-elämän välillä? Juuri siitä tässä Data Detoxin osiossa on kyse.

Aloitetaan!

Tuotteen takana
TACTICAL TECH

Tukijana
Firefox

datadetoxkit.org
#datadetox

1.

OLE LÄSNÄ TÄSSÄ HETKESSÄ

Tämä vinkki on vaikeampi toteuttaa kuin miltä se kuulostaa. Hetkessä eläminen vaatii päivittäistä harjoittelua. Se on kuin aivojen lihas, jota sinun on harjoitettava säännöllisesti. Voit aloittaa pohtimalla suhdettasi käyttämääsi teknologiaan.

Kuinka paljon aikaa vietät puhelimesi kanssa?

Jos et ole tyytyväinen vastaukseen, on olemassa asetuksia ja strategioita, joiden avulla voit hallita teknologian käyttöäsi paremmin.

Jos tavoitteesi on viettää vähemmän aikaa Facebookissa, Instagramissa tai Snapchatissa, muuta sovellusten asetuksia ja käyttöoikeuksia, jotta ne sopivat paremmin juuri sinulle. Jotkut sovellukset, kuten Instagram, jopa tarjoavat palvelun, jonka avulla sovellus muistuttaa sinua, kun päivittäinen aikarajasi on saavutettu.

Instagram:
Profiili → valikko →
Asetukset → Käyttäjätili →
Sinun toimintasi →
Aseta päivittäinen muistutus

Jos puhelimesi häiritsee tosielämässä käymiäsi keskusteluja soimalla, piippaamalla tai välähtelemällä, voit hiljentää sen väliaikaisesti, asettaa puhelimen pöydälle näyttöpuoli alaspäin tai jopa työntää sen taskuusi tai laukkuusi, jotta et näe sitä.

2.

HUOMAA SUUNNITTELUTEMPUT

Suostuttelevalla suunnittelulla, joka tunnetaan myös nimellä harhaanjohtava suunnittelu (dark patterns), tarkoitetaan suunnittelua, joka perustuu ihmisen psykologiaan. Sitä käytetään provosoimaan sinut rekisteröitymään johonkin, ostamaan jotain tai luovuttamaan enemmän henkilökohtaisia tietoja kuin luulit tai tarkoitit antavasi.

Yleisimmät suostuttelevan suunnittelun keinot voivat sisältää tiettyjen värien käyttöä, painikkeiden sijoittelua, epäselviä tekstejä tai puutteellisia tietoja. Joskus nämä temput ovat ilmiselviä, mutta toisinaan niitä on vaikea havaita. Olet ehkä jo huomannut joitakin näistä vaikkapa tilatessasi uutiskirjeen tai tehdessäsi verkko-ostoksia.

Voit olla sovelluksia fiksumpi monella eri tapaa.

Tunnista suostuttelu: Ensimmäinen asia, jonka voit tehdä, on yksinkertaisesti olla tietoinen näiden tekniikoiden käytöstä.

Ota kuvakaappaus ja jaa: Ota kuvakaappauksia aina, kun näet suostuttelevaa suunnittelua verkossa, ja jaa ne ystäviesi kanssa (ilman henkilökohtaisia tietoja, muista tietosuoja!). Voit myös pyytää yrityksiä muuttamaan käytäntöjään.

Pysy rauhallisena: Jos ostosivulla tikittää lähtölaskenta, kysy itseltäsi: onko minulla todellakin kiire? Jos kuitenkin napsautat, vaikket oikeastaan olisi halunnut, mieti napsauttamasi painikkeen tekstin sanamuotoa tai palvelussa käytettyjä värejä. Jos olet hämmentynyt, älä ajattele vian olevan itsessäsi – mieti verkkosivuston tai sovelluksen käyttämiä sanoja, sillä ne saattavat olla epäselviä.

3.

YMMÄRRÄ MEDIAA

Sen lisäksi, että voit oppia olemaan fiksumpi kuin ne ominaisuudet ja mallit, joiden on tarkoitus pitää sinut vierittämässä sivuja ja napsauttelemassa kohteita, voit myös olla haka harhaanjohtavien uutisten tai viestien havaitsemisessa.

Tähän mennessä olet todennäköisesti kuullut vääriä tietoja ja valeuutisia koskevista ongelmista. Voit tulla tietoiseksi vääristä tiedoista, jos otat tavaksi kysyä kriittisiä kysymyksiä kaikista lukemistasi ja näkemistäsi uutisista, varsinkin jos uutinen näyttää yllättävältä, sokeeraavalta tai liian hyvältä ollakseen totta.

Aina kannattaa varmistaa, mitkä uutiset ovat todellisia ja mitkä väärennettyjä, varsinkin jos aiot jakaa ne perheesi tai ystäviesi kanssa.

Miltä verkkosivustolta tämä on peräisin?
Kuka kirjoitti sen (ja milloin)?
Mitä koko artikkeli käsittelee, otsikon lisäksi?
Mihin lähteisiin artikkelissa viitataan?

Jos luulet uutisen olevan väärää tietoa ja haluat estää sen leviämisen, useimmat alustat tarjoavat mahdollisuuden raportoida tällaisista uutisista. Voit myös miettiä, haluatko jatkaa uutisen jakaneen tilin seuraamista.

5.

ETSI TOTUUS VERKOSTA

Valeuutiset-termillä viitataan erilaisiin epätarkkoihin tai harhaanjohtaviin tietoihin. Esimerkiksi satiiri, huonosti tutkittu tai vahvistamaton sisältö, huijaukset ja petokset saattavat sisältää tällaisia tietoja. Valeuutisia ei aina levitetä vahingoittamistarkoituksessa. Riippumatta jakamisen syistä tulos on kuitenkin yleensä sama: uutisen vastaanottavat ihmiset uskovat, että jokin vale on oikeasti totta tai että tapahtui jotakin, mitä ei tosiasiassa koskaan tapahtunut.

Parhaimmillaan se voi olla hauska meemi. Pahimmillaan se voi olla virheellistä terveystietoa tai väärää poliittista tietoa.

Vaikka kuinka yrittäisit tutkia ja esittää kriittisiä kysymyksiä lukemistasi artikkeleista, saatat silti olla hämmentynyt. Muista kuitenkin: et ole yksin!

Kaikkien panosta tarvitaan
Vaikkei verkkosivusto tunnustaisi omia virheitään, ei se tarkoita sitä, että se ei tekisi niitä. Itse asiassa luotettavimmat julkaisut ovat erityisen varovaisia totuuden suhteen, ja ne työllistävät ihmisiä tai kokonaisia osastoja, joiden ainoa tehtävä on faktojen tarkastaminen.

Etsi lähteitä, jotka korjaavat virheensä. Vielä parempi, jos korjaus mainitaan artikkelin alussa ja jaetaan sosiaalisessa mediassa, joten se ei ole turhan hankalasti löydettävissä.

6.

PUHKAISE KUPLASI

Kun verkkosivustot ja sovellukset ovat rakentaneet kiinnostuksen kohteittesi perusteella sinusta profiilin, saatat saatat joutua ns. suodatinkuplaan. Tällöin palvelut tarjoavat sinulle lisää samanlaisia tarinoita, joita olet napsauttanut aiemmin. Kuinka tämä käytäntö rajoittaa tai muuttaa sitä, mistä kuulet ja mitä näet?

Suodatinkuplaan päätyminen voi saada ihmiset näkemään täysin erilaisia tarinoita, uutisotsikoita, artikkeleita ja mainoksia, kuten interaktiivinen artikkeli Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed) osoittaa.

Jos tiedät, että katselet algoritmisesti kuratoitua sisältöä, joka on suunniteltu erityisesti sinulle käyttämissäsi sovelluksissa ja verkkosivustoilla, seuraa kysymys: kuinka voit rikkoa kuplasi?

Anna muutoksen tuulien puhaltaa ja sekoita uutissisältöä
Hyvä tapa räjäyttää suodatinkupla on tilata palveluita, jotka kokoavat uutisia ja tietoja useista lähteistä ja monipuolisista näkökulmista. Sellaiset RSS-syötteet, foorumit ja postituslistat, jotka jakavat tietoja monista eri näkökulmista ja teemoista, voivat auttaa sinua näkemään maailman kuplasi ulkopuolella. Voit aloittaa lukemalla vaikkapa Global Voices (globalvoices.org) -sivustoa ja The Syllabus (the-syllabus.com) -sivustoa.

DATA DETOX KIT

6 VINKKIÄ VÄÄRÄN TIEDON VÄLTTÄMISEKSI VERKOSSA

Sovellukset, verkkosivustot ja verkkomedia saattavat olla välttämättömiä, kun haluat lukea uutisia, etsiä elämää helpottavia vinkkejä tai nauttia viihteestä. Mutta kaiken sisällön keskellä voi olla hankalaa löytää juuri se tieto, jota etsit.

Lisäksi voi olla vaikea erottaa fakta ja fiktio verkkovideoista, -kuvista tai -artikkeleista. Persoonallisuustestit, jotka yrittävät profiloida sinua, järkyttävät otsikot ja muokatut valokuvat tai videot, jotka saattavat vakuuttaa sinut täysin toisenlaisesta todellisuudesta, ovat esimerkkejä siitä, että verkossa näkemäsi asiat eivät aina ole sitä miltä näyttävät.

Tässä Data Detox -osiossa tutkitaan väärää tietoa koskevia aiheita ja trendejä. Aloitamme tutustumalla tarkemmin jokaisen omaan vastuuseen ja sen jälkeen käsittelemme aihetta laajemmin. Samalla annamme neuvoja, miten navigoida kaiken tämän keskellä.

Aloitetaan!

datadetoxkit.org **#datadetox**

Tuotteen takana
TACTICAL TECH

Yhteistyökumppanit:
Save the Children 100 ANNI
IFLA

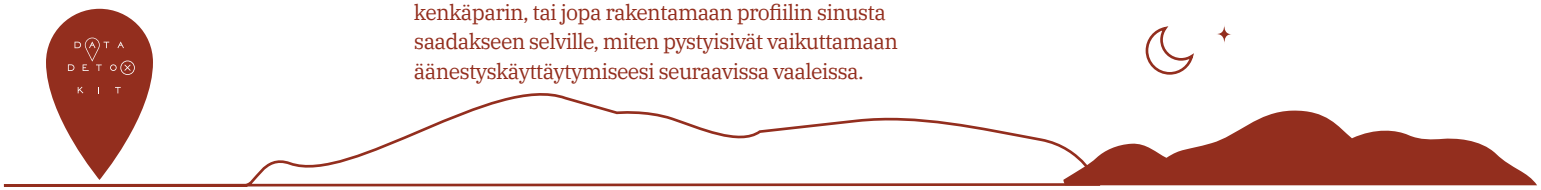
Rahoittajana Euroopan unioni

1.

YMMÄRRÄ OMAN VAIKUTUKSESI MERKITYS

Tykkääminen, jakaminen, uudelleentwiittaminen ja edelleenjakaminen ovat kaikki tapoja olla vuorovaikutuksessa verkossa näkemiesi asioiden kanssa, ja sinun tekemisilläsi on suuri vaikutus. Kun tarpeeksi moni ihminen näkee kuvan, videon tai postauksen, se leviää nopeasti ja muuttuu ns. viraaliksi.

Pysähdy hetkeksi ja kysy itseltäsi: **Miten minä vaikutan verkossa?** Milloin viimeksi olen lähettänyt näkemäni järkyttävän tai hauskan artikkelin, otsikon, videon tai kuvan vain muutamassa sekunnissa ystävilleni? Tutkijat ovat havainneet, että viraaleiksi päätyvät tarinat ja kuvat ovat todennäköisimmin niitä, jotka saavat sinut tuntemaan pelkoa, inhoa, kunnioitusta, vihaa tai ahdistusta. Jos teit juuri näin tänä aamuna, älä huoli!



Jakaminen on välittämistä
Jakaminen on tapa osallistua. Kun jaat jotain (mitä tahansa), mahdollistat julkaisun muuttumisen viraaliksi. Entä jos se osoittautuukin esimerkiksi valeuutiseksi, haluatko todella, että nimesi ja maineesi liitetään siihen? Ennen kuin jaat linkin, mieti, levitätkö jotakin valheellista, tuhoavaa tai vihamielistä.

2.

HARKITSE TARKKAAN ENNEN KUIN TEET PERSOONALLISUUSTESTIN

Milloin viimeksi näit testin (joko teksti- tai valokuvasuodattimissa), jonka avulla saisit selville esimerkiksi

- mikä vuosikymmen olet
- mikä on voimaeläimesi
- ja niin edelleen ja niin edelleen!

Vaikka on täysin mahdollista, että testi on vain hauska ja suunniteltu viihteeksi, on myös mahdollista, että kysymykset on muotoiltu huolellisesti keräämään tietoja persoonallisuutesi luokittelemiseksi ns. psykometristen mallien mukaisesti.

Vastauksesi vaikkapa Mikä Simpsonien hahmo olet? -testiin ja muut tavat, joita selaimet, sovellukset tai muut liitetyt tuotteet, kuten kanta-asiakaskortit, valvovat, voivat antaa analyytikoille käsityksen siitä, millainen henkilö olet ja mistä asioista välität. Näin ne pystyvät vaikuttamaan siihen, että ostat esimerkiksi kenkäparin, tai jopa rakentamaan profiilin sinusta saadakseen selville, miten pystyisivät vaikuttamaan äänestyskäyttäytymiseesi seuraavissa vaaleissa.

Pidä salaisuudet salaisuuksina
Kun ajattelet yksityisiä tietoja, ensimmäisenä mieleesi tulevat varmasti salasanat, henkilötunnus ja pankkitilin numero. Pelkosi, ärsytyksen aiheesi tai tavoitteesi ovat kuitenkin myös yhtä henkilökohtaisia asioita. Data-analyytikot pitävät näitä yksityiskohtia arvokkaina tietoina, jotka kertovat sinusta ihmisenä. Harkitse tarkasti aina, ennen kuin annat tällaisia tietoja itsestäsi kyselyiden tai persoonallisuustestien avulla.

3.

ÄLÄ TARTU SYÖTTIIN

Klikkiotsikko on termi, jota käytetään kuvaamaan sensaatiomaisia, epärehellisiä tai keksittyjä otsikoita, joiden tarkoituksena on provosoida ihmisiä napsauttamaan otsikkoa tai linkkiä. Mitä enemmän huomiota artikkeli, video tai kuva kerää, sitä enemmän rahaa sen avulla todennäköisesti ansaitaan. Tämä tarkoittaa sitä, että sisällöntuottajien tarkoituksena on sanoa mitä tahansa, jotta napsautat tai jaat heidän sisältöään.

Käyttämäsi alustat (kuten Facebook ja Instagram) luovat sinusta henkilöprofiilin,. Sen perusteella saatat saada räätälöityjä otsikoita, jotka on luotu aiheuttamaan sinussa tuntemuksia, jotka puolestaan todennäköisesti saavat sinut napsauttamaan otsikkoa.

Klikkiotsikoita voi esiintyä myös väärien tietojen yhteydessä, mutta ei aina. Kun alat tunnistaa klikkiotsikoita, huomaat, että niitä on kaikkialla: YouTubessa, blogeissa ja iltapäivälehdissä.

Etsi tietojen lähde
Kun törmään klikkiotsikkoon, älä katso pelkkää otsikkoa. Jos linkki näyttää turvalliselta, napsauta artikkelia ja selvitä, kuka jutun kirjoitti, milloin se julkaistiin ja mihin lähteisiin siinä viitataan. Voi olla, että artikkeli sisältää huomautuksen maksetusta sisällöstä tai mainoksista, tai se saattaa olla luokiteltu mielipidekirjoitukseksi. Nämä yksityiskohdat voivat auttaa päättämään, onko koko juttu jakamisen arvoinen.

4.

VARO VÄÄRENNÖKSIÄ

Deep fakes eli koneelliset väärennökset ovat videoita, äänileikkeitä tai kuvia, joita on muutettu digitaalisesti, tyypillisesti korvaamaan jonkun kasvot tai liikkeet tai muuttamaan heidän sanojaan. Vaikka deep fakes on uusi termi, tällaisia väärennöksiä on oikeastaan ollut olemassa muodossa tai toisessa kautta aikojen. Niin sanottujen halpojen väärennösten luominen on vieläkin helpompaa. Ne ovat harhaanjohtavaa sisältöä, joka ei vaadi kehittynyttä tekniikkaa, vaan luodaan yksinkertaisesti lisäämällä väärä otsikko valokuvaan tai videoon tai käyttämällä vanhentunutta sisältöä kuvaamaan nykyistä tapahtumaa.

Saattaa tuntua mahdottomalta todella torjua väärennöksiä, mutta voit tehdä jotakin hyvin tärkeää: pidä jalat maassa.

Pidä jalat maassa ja perehdy asioihin
Aivan kuten klikkiotsikoidenkin kohdalla, älä usko kaikkea. Jos näkemäsi video tai valokuva näyttää yllättävältä tai sokeeraavalta, tunnista tunteesi ja mieti, onko asiassa koira haudattuna. Jos huomaat, että näet saman kuvan useasti tai se on jaettu sinulle useita kertoja, on ehkä syytä etsiä kuvan oikea lähde.

Silloin on syytä kysyä tarkennuksia: kuka tämän julkaisi (mikä verkkosivusto, kuka on tekijä)? Milloin se julkaistiin? Jos kyseessä on kuva, tee käänteinen kuvahaku TinEye -sivustolla ja katso, mistä muualta kuva löytyy.

Tarkista muut uskottavat uutislähteet ennen kuin pidät sitä totena ja jaat sen ystävillesi ja perheellesi.